# Simplifying **Shared Responsibility** on Microsoft Azure

HOW ARMOR ANYWHERE HELPS YOU SECURE AND OPTIMIZE YOUR AZURE INSTANCES

THE FIRST TOTALLY SECURE CLOUD COMPANY™

Microsoft Azure

ARMOR™

# Introduction

Modern organizations want to take advantage of Microsoft Azure's Infrastructure as a Service (IaaS) offering to host their applications, data and systems in a modern public cloud. Azure provides incredible flexibility and scalability for its customers, who can increase or decrease their use of Azure processing, storage, networking and other resources immediately at any time. While the benefits are obvious, one critical question remains for organizations migrating to Azure: **how is it secured?**

Per the Azure Shared Responsibility Model, security is shared between Azure and their customers. Azure manages security controls of its IaaS infrastructure, while all tasks pertaining the hosted data and applications are handled by the customer.

While an effective model for managing the nuances of public cloud security, fulfilling the shared responsibility model is a major undertaking for most organizations– especially for those lacking the resources (both in terms of personnel and technology) to adequately secure their cloud data and applications.

Without proper guidance and support from a proven security provider, these organizations face the prospect of being solely responsible for their portion of shared responsibility on Azure.

# Armor Anywhere for Azure

This is where Armor steps in. Our managed cloud security solution, Armor Anywhere, helps Azure customers reduce the burden of shared responsibility while optimizing their public cloud environment.

Installed in an Azure environment through a single agent, Armor Anywhere empowers Azure customer to leverage multiple best-of-breed security tools, merging them seamlessly with Microsoft native platforms such as OMS and Azure Security Center (ASC).

It delivers a live view of each Azure instance to the analysts in the Armor 24/7/365 security operations center (SOC), which in turn enables organizations to scale infrastructure without impact to security, compliance or agility. Armor Anywhere leverages a full API stack enabling seamless integration with ASC, OMS or existing security operations.

This solution provides simplicity, dev-ops friendliness and scalability while allowing Azure customers to maintain focus on delivering security and compliance outcomes without sacrificing any of the benefits of moving to the Azure cloud.

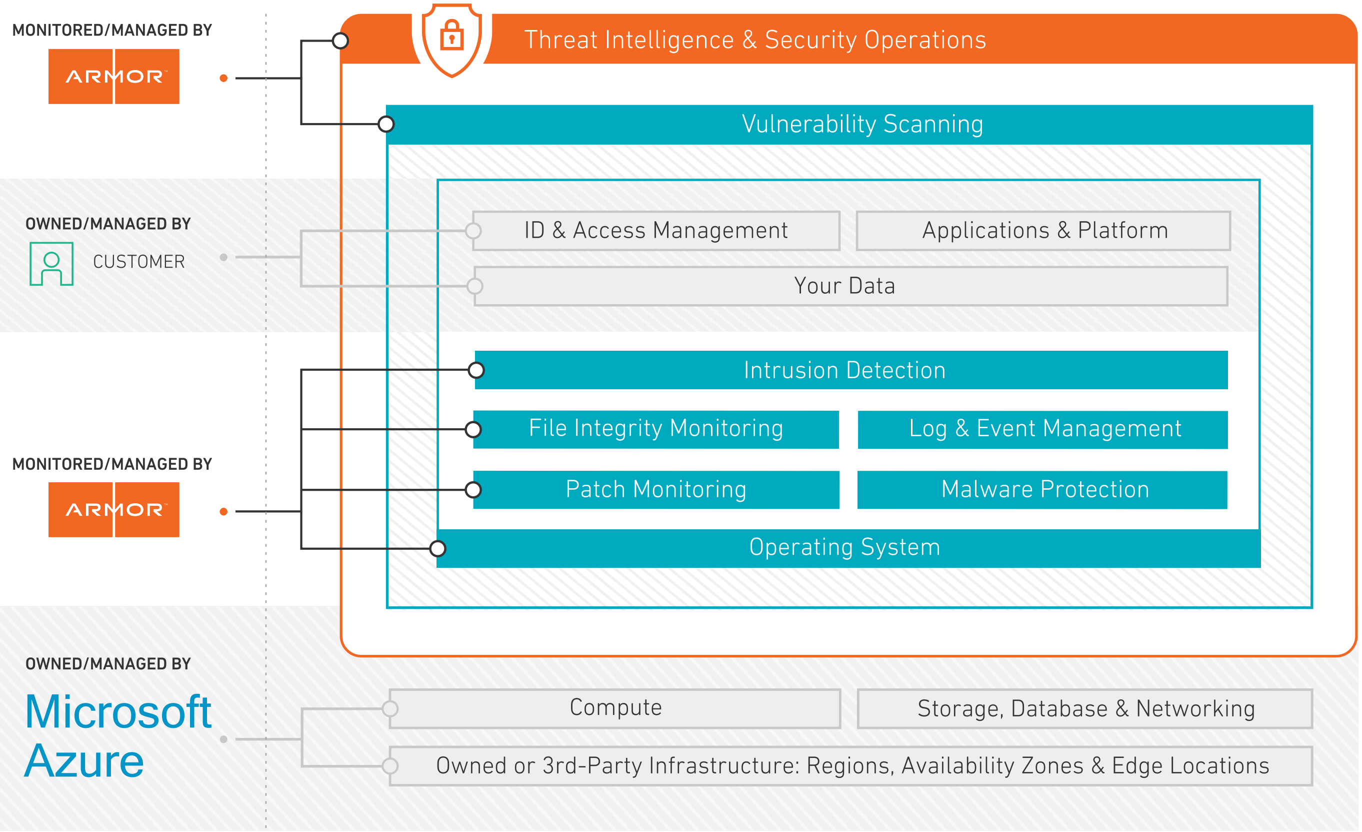
## In-depth: Shared Responsibility on Armor Anywhere

This white paper outlines how Armor Anywhere delivers these benefits and actively streamlines the responsibilities Azure customers are required to fulfill according to Microsoft's Shared Responsibility Model.

For more information regarding Armor Anywhere or to request a demo, visit armor.com/armor-anywhere-security/

# A Closer Look at the Shared Responsibility Model

This graphic shows Armor Anywhere's role within the shared responsibility model for Azure security. It groups the responsibilities into four layers with the responsible party identified on the left side for each layer. Let's walk through those layers from bottom (cloud infrastructure) to top (security operations center).



## Azure Responsibilities

**Azure security responsibilities fall into three categories:**

- **Physical security:** Azure provides a wide range of physical security controls for its facilities, everything from monitoring facility premises with guards, cameras and sensors to restricting who can access the facilities and what each person can access within each facility.

- **Network security:** Azure enforces a small number of network security controls, but each control is important. One example is the detection and mitigation of distributed denial of service (DDoS) attacks, whether these attacks originate from external locations or from an Azure customer's instance. Another example is the network isolation of each Azure customer from all other Azure customers by default. In other words, Azure customer A's instance can't establish a network connection to Azure customer B's instance without B's prior approval.

- **Virtual infrastructure security:** Azure ensures that its virtual infrastructure is secured, because, if breached, it could allow an attacker to compromise several customer VM instances at once. Responsibilities in this category include managing hypervisor security, such as applying hypervisor patches and maintaining a secure hypervisor configuration as well as periodically releasing updated VM images that incorporate the latest patches.

## Armor Anywhere Responsibilities inside the Azure Instance

**In the shared responsibility model, Armor Anywhere takes care of two layers, one supporting security inside the instance and the other supporting security outside the instance. In this layer, inside the instance, Armor Anywhere responsibilities are as follows:**

- **File integrity monitoring:** Armor Anywhere monitors the operating system's critical files to identify any changes to those files, then determines if those changes are known to be benign, such as the result of installing a new patch. Any files with unexplained changes cause Armor Anywhere to generate an alert so that staff can investigate the changes, determine the source, and initiate incident response processes if needed.

- **Log and event management:** Another important responsibility handled by Armor Anywhere is log and event management. Armor Anywhere collects security-related operating system event information from logs, then makes that log information available through the Armor Management Portal (AMP). AMP provides a single place for viewing and querying the log information across all Azure instances. Armor Anywhere also takes care of log retention duties to ensure that the necessary information is available to support compliance initiative reporting.

- **Patch monitoring:** Armor Anywhere frequently checks each customer Azure instance to identify any missing operating system patches. The customer is immediately notified of any missing patches, and staff can use AMP to view the information on missing patches, including which patches are missing for each instance and what actions are required for each patch, such as rebooting the operating system after patch installation.

- **Managed malware protection:** Another feature of Armor Anywhere is that it provides managed malware protection within each organization's Azure instances. This protection looks for a range of malware attempting to infect the operating systems within the Azure instances. If Armor Anywhere finds malware, it will notify Armor experts for follow up with the customer.

Microsoft Azure | ARMOR™

## Customer Responsibilities

**The next layer in the shared responsibility model belongs to the customer. The details of these will be unique for each organization, but at a high level they usually include the following:**

- **Identity and access management:** This involves managing the identities used to authenticate users, administrators, services, devices, and any other entity. In addition, the customer must also manage the authentication mechanisms used to verify claimed identities, as well as to use access control lists and other methods of specifying the rights and privileges for each identity.
- **Application and platform security:** Application and platform security encompasses several security controls, including change management processes for software patches and configuration settings, software vulnerability assessment and application-specific protection, such as Web application firewalls. Additionally, customers may need to ensure that only the necessary network connectivity is permitted between the customer's instances. The overall goals for application and platform security are to minimize vulnerabilities in the operating system and applications, and to detect and potentially stop attacks attempted against the operating system and applications.
- **Data security:** The importance of data security is wholly dependent on the sensitivity of the data being stored or processed within a customer's instances. If sensitive data is present, examples of possible security controls include storage encryption technologies to safeguard the confidentiality of the data, and data loss prevention (DLP) technologies to identify attempts to inadvertently or intentionally exfiltrate the data. However, even if sensitive data is not present in the traditional sense, there still may be passwords, cryptographic keys, or other customer system security data that must be protected.

## Armor Anywhere Responsibilities Outside the Instance

**The outermost layer in the shared responsibility model is handled by Armor Anywhere. The security controls in this layer essentially wrap around the other security controls sitting on top of the Azure cloud infrastructure. This layer includes the following:**

- **External vulnerability scans:** To complement vulnerability scans of each customer instance, Armor Anywhere performs routine vulnerability scans from an external point of view. They reveal which vulnerabilities are readily visible to external attackers, making them more likely to be targeted.
- **Managed security operation center services:** Armor experts monitor security operations for Armor Anywhere customers around the clock. For example, when they see a major security problem require a rapid response, they notify the customer immediately.
- **Threat intelligence:** Because Armor Anywhere is used to monitor security operations for customers around the world, Armor is always seeing the latest threats and gathering information on them. This threat intelligence is then utilized for all Armor Anywhere customers to improve protection and detection capabilities.

# Advantages of an Armor Anywhere on Azure

There are four main advantages of using Armor to help secure an organization's new and existing Azure instances:

ARMOR™
THE FIRST TOTALLY SECURE CLOUD COMPANY™

### Flexibility

Leverage Azure's capabilities, including its flexibility and scalability while ensuring that the security of data, applications, and operating systems are maintained.

### Consolidated View

Organizations can save a great deal of time and effort by using Armor Anywhere agents to handle numerous security monitoring functions, as well as log management and malware protection, instead of having to evaluate, select, acquire, deploy, configure, monitor and maintain all those security controls in-house.

### Managed Security

When an Armor Anywhere agent detects a potentially serious security event within any Azure instance, our experts quickly analyze the information and contact customers if immediate action is needed to safeguard data or applications.

### Lower TCO

Armor Anywhere helps organizations achieve a lower total cost of ownership for IaaS cloud usage compared to do-it-yourself security solutions and even other managed security services.

**For more information on Armor and its partnership with Azure, visit - https://www.armor.com/azure/**

Microsoft Azure | ARMOR